

On the Security of Millimeter Wave Vehicular Communication Systems using Random Antenna Subsets

Mohammed E. Eltayeb, Junil Choi, Tareq Y. Al-Naffouri*, and Robert W. Heath, Jr.

The University of Texas at Austin, Emails: {meltayeb,junil.choi,rheath}@utexas.edu.

*King Abdullah University of Science and Technology, Email: tareq.alnaffouri@kaust.edu.sa

Abstract—Millimeter wave (mmWave) vehicular communication systems have the potential to improve traffic efficiency and safety. Lack of secure communication links, however, may lead to a formidable set of abuses and attacks. To secure communication links, a physical layer precoding technique for mmWave vehicular communication systems is proposed in this paper. The proposed technique exploits the large dimensional antenna arrays available at mmWave systems to produce direction dependent transmission. This results in coherent transmission to the legitimate receiver and artificial noise that jams eavesdroppers with sensitive receivers. Theoretical and numerical results demonstrate the validity and effectiveness of the proposed technique and show that the proposed technique provides high secrecy throughput when compared to conventional array and switched array transmission techniques.

Index Terms—Millimeter-wave, PHY security, beamforming, V2X.

I. INTRODUCTION

Future intelligent transportation systems (ITSs) will rely on vehicular communication technologies to enable a variety of applications for safety, traffic efficiency, driver assistance, and infotainment [1], [2]. The abundance of bandwidth in the millimeter wave (mmWave) will enable higher data rate communication between vehicles to exchange the raw data from LIDAR, radar, and other sensors to support advanced driver-assisted and safety-related functionalities.

Like regular communication systems, vehicular communication systems are prone to a set of abuses and attacks that could jeopardize the efficiency of transportation systems and the physical safety of vehicles and drivers. Security threats and attacks in vehicular environments have been described in detail in [2]–[6]. To preserve the privacy and security of vehicular communication networks, higher-layer encryption techniques have been proposed in [6]–[8], and references therein. These techniques, however, are based on digital signature methods that require vehicles to store large number of encryption keys. These keys must also be regularly exchanged, hence creating, in addition to the processing overhead, an additional communication overhead [1], [2]. With the emergence of new time-sensitive ITS applications and the increasing size of the decentralized vehicular network, the implementation of these higher-layer techniques becomes complex and challenging. Additionally these techniques fail to secure communication links if the encryption keys are compromised, and/or key distribution becomes difficult.

To mitigate these challenges, *keyless* physical layer (PHY) security techniques [9]–[20], which do not directly rely on upper-layer data encryption or secret keys, can be employed to secure vehicular communication links. These techniques are based on the use of one or more of the following approaches: (i) directional beamforming [10]–[13], (ii) distributed arrays (or nodes) [14] [15], (iii) dual-beam techniques [16], and (iv) switched arrays [17]–[20]. In all of these techniques, the transmitter uses multiple antennas to create interference or *artificial noise* within the null space of the receiver. Such interference will degrade the channel of potential eavesdroppers and will not impact the receiver’s channel.

Despite their effectiveness, the techniques in [10]–[16] require fully digital baseband precoding, which is difficult to realize in mmWave vehicular systems. This is due to the limited number of available RF chains and additional hardware and power constraints in mmWave systems [21] [22]. While it might be justifiable to deploy large number of RF chains in cellular base stations with relaxed power constraints, this leverage might not be possible in vehicular transmitters. Due to both power and hardware constraints, switched array techniques [17]–[20] might be suitable for vehicular mmWave systems with large number of antennas. These techniques use antenna switches to associate a subset of antennas with every transmission symbol. This results in coherent transmission towards the receiver and induces artificial noise in all other directions. Nonetheless, it was recently shown that switched array security techniques can be breached by exploiting the sparsity in the transmit antenna array [23] [24].

In this paper, we propose a new PHY security technique for vehicular communications that does not require the exchange of keys between vehicles. We assume a single transmitter communicating with a single receiver in the presence of an eavesdropper as shown in Fig. 1. The proposed technique uses an antenna architecture with a single RF chain (instead of multiple RF chains), and performs analog precoding with antenna selection. To transmit an information symbol, a random set (called a subset) of antennas are co-phased to transmit the information symbol to the receiver, while the remaining antennas are used to randomize the far field radiation pattern at non-receiver directions. This results in coherent transmission to the receiver and a noise-like signal that jams potential eavesdroppers with sensitive receivers. Note that the proposed technique is robust to plaintext attacks and

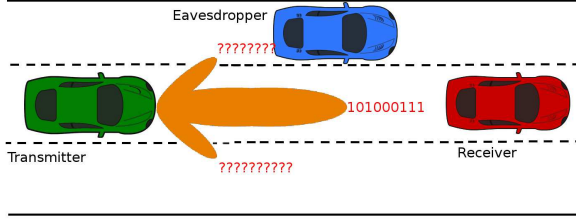


Fig. 1: Vehicle to vehicle communication with a possible eavesdropper. The transmitting vehicle is communicating with a target vehicle while the eavesdropper tries to intercept the transmitted data.

other attacks highlighted in [23] and [24] since a random subset is associated with every data symbol, and all antennas are used for data transmission, i.e. the array is no longer sparse.

II. SYSTEM MODEL

We consider a mmWave system with a transmitting vehicle (transmitter) and a receiving vehicle (receiver) in the presence of a single or multiple eavesdroppers as shown in Fig. 1. The transmitter is equipped with N_T transmit antennas and a single RF chain as shown in Fig. 2. The receiver is equipped with N_R antennas. We adopt a uniform linear array (ULA) with isotropic antennas along the x-axis with the array centered at the origin; nonetheless, the proposed technique can be adapted to arbitrary antenna structures. Since the array is located along the x-y plane, the receiver's location is specified by the azimuth angle of arrival/departure (AoA/AoD). The transmitter is assumed to know the angular location of the target receiver but not of the potential eavesdroppers.

The transmit data symbol $s(k) \in \mathbb{C}$, where $\mathbb{E}[|s(k)|^2] = 1$ and k is the symbol index, is multiplied by a unit norm transmit beamforming vector $\mathbf{f} = [f_1 \ f_2 \ \dots \ f_{N_T}] \in \mathbb{C}^{N_T}$ with f_n denoting the complex weight on transmit antenna n . At the receiver, the received signals on all antennas are combined with a unit norm receive combining vector $\mathbf{w} = [w_1 \ w_2 \ \dots \ w_{N_R}] \in \mathbb{C}^{N_R}$. Assuming a narrow band line-of-sight (LOS) channel with perfect synchronization, the received signal can be written as

$$y(k, \phi, \theta) = \sqrt{P\alpha} \mathbf{w}^* \mathbf{H}(\phi, \theta) \mathbf{f} s(k) + z(k), \quad (1)$$

where ϕ is AoA at the receiver and θ is AoD from the transmitter, P is the transmission power and α is the path-loss. In (1), \mathbf{H} is the $N_R \times N_T$ channel matrix that represents the mmWave channel between the transmitter and the receiver, and $z(k) \sim \mathcal{CN}(0, \sigma^2)$ is the additive noise.

Due to the dominant reflected path from the road surface, a two-ray model is usually adopted in the literature to model LOS vehicle-to-vehicle communication [26]-[28]. Based on this model, the channel \mathbf{H} can be modeled using array manifold concepts as $\mathbf{H} = g \mathbf{a}_r(\phi) \mathbf{a}_t^*(\theta)$, where $g = \frac{1}{\sqrt{2}}(1 + r e^{j\Phi})$, $r = -1$ is the reflection coefficient of the road, and Φ is the angle between the direct and the reflected path and it is given by $\Phi = \frac{2\pi}{\lambda} \frac{2h_t h_r}{D}$ [28]. The variables h_t , h_r represent the height of the transmitting and receiving antennas respectively, D is

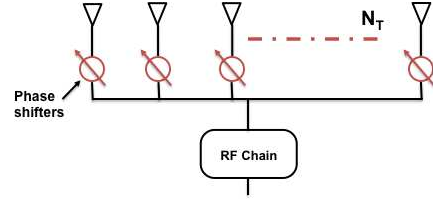


Fig. 2: Array architecture with N_T antennas and a single RF chain.

the distance between the vehicles, and λ is the wavelength. Since $h_t h_r \ll D$, which is typical in vehicular environments, the angle Φ is small and both the LOS and non-LOS paths combine at the azimuth AoA ϕ . The vector $\mathbf{a}_r(\phi)$ represents the receiver's array manifold corresponding to the AoA ϕ and the vector $\mathbf{a}_t(\theta)$ represents the transmitter's array manifold corresponding to the AoD θ . For simplicity, the receiver's beam is assumed to be aligned to towards the transmitter for maximum reception i.e. $\mathbf{w} = \mathbf{a}_r(\phi)$. Hence, the received signal along an angle θ becomes

$$y(k, \theta) = \sqrt{P\alpha} \mathbf{a}_r^*(\phi) \mathbf{H}(\phi, \theta) \mathbf{f} s(k) + z(k) \quad (2)$$

$$= \sqrt{P\alpha N_R} \mathbf{h}^*(\theta) \mathbf{f} s(k) + z(k), \quad (3)$$

where N_R is the array gain at the receiver. For a ULA with $d \leq \frac{\lambda}{2}$ antenna spacing, the channel for a receiver located along the θ direction can be written as $\mathbf{h}^*(\theta) = g[e^{-j(\frac{N-1}{2})\frac{2\pi d}{\lambda} \cos \theta} \ e^{-j(\frac{N-1}{2}-1)\frac{2\pi d}{\lambda} \cos \theta} \ \dots \ e^{j(\frac{N-1}{2})\frac{2\pi d}{\lambda} \cos \theta}]$ [29].

III. MILLIMETER WAVE SECURE TRANSMISSION

In this section, we introduce a novel analog PHY security technique that randomizes the data stream at the eavesdropper without the need for a fully digital array or antenna switches as done in [11]-[20]. Instead of using all antennas for beamforming, a set of random antennas are used for coherent beamforming, while the remaining antennas are set to destructively combine at the receiver. The indices of these antennas are randomized in every symbol transmission. This randomizes the beam pattern sidelobes and as a result, produces noise-like signals at non-receiver directions. Although the target receiver would observe a fixed gain reduction (due to destructive combining), malicious eavesdroppers will observe a noise-like interference.

Let $\mathcal{I}_M(k)$ be a random subset of M antennas used to transmit the k th symbol, $\mathcal{I}_L(k)$ be a subset that contains the indices of the remaining antennas, $\mathcal{E}_L(k)$ be a subset that contains the even entries of $\mathcal{I}_L(k)$, and $\mathcal{O}_L(k)$ be a subset that contains the odd entries of $\mathcal{I}_L(k)$. The progressive inter-antenna phase shifts are set as

$$\Upsilon_n(k) = \begin{cases} \Psi_n(k), & n \in \mathcal{I}_M(k) \\ \Psi_n(k), & n \in \mathcal{E}_L(k) \\ -j \log(-e^{j\Psi_n(k)}), & n \in \mathcal{O}_L(k) \end{cases} \quad (4)$$

where $\Psi_n(k) = (\frac{N-1}{2} - n) 2\pi \frac{d}{\lambda} \cos(\theta_R)$, and θ_R is the transmit direction towards the legitimate receiver. Note in (4) $e^{j(-j \log(-e^{j\Psi_n(k)}))} = -e^{j\Psi_n(k)}$, and the n th entry of the

beamforming vector $\mathbf{f}(k)$ is $f_n(k) = \frac{1}{\sqrt{N_T}} e^{j\Upsilon_n(k)}$. Using (3) and (4), the received signal at the receiver along θ_R becomes

$$y_R(k, \theta_R) = \sqrt{\frac{P\alpha N_R}{N_T}} g_R s(k) \times \left(\sum_{m \in \mathcal{I}_M(k)} e^{-j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} \cos \theta_R} e^{j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} \cos \theta_R} + \sum_{n \in \mathcal{E}_L(k)} e^{-j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} - \sum_{n \in \mathcal{O}_L(k)} e^{-j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} \right) + z(k), \quad (5)$$

where g_R is the channel gain at the receiver, N_R is the receiver's array gain, and N_T is a power normalization term. Grouping similar terms in (5) we obtain

$$y_R(k, \theta_R) = s(k) g_R \sqrt{\frac{P\alpha N_R}{N_T}} \times \left(\sum_{m \in \mathcal{I}_M(k)} e^{j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} (\cos \theta_R - \cos \theta_R)} + \sum_{n \in \mathcal{E}_L(k)} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} (\cos \theta_R - \cos \theta_R)} - \sum_{n \in \mathcal{O}_L(k)} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} (\cos \theta_R - \cos \theta_R)} \right) + z(k) \\ = \underbrace{s(k)}_{\text{information symbol}} \underbrace{g_R \sqrt{P\alpha}}_{\text{effective channel gain}} \underbrace{M \sqrt{\frac{N_R}{N_T}}}_{\text{array gain}} + \underbrace{z(k)}_{\text{additive noise}}. \quad (6)$$

Similarly, the received signal at the eavesdropper can be written as

$$y_E(k, \theta_E) = \sqrt{\frac{P\alpha_E N_E}{N_T}} g_E s(k) \times \left(\sum_{m \in \mathcal{I}_M(k)} e^{-j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} \cos \theta_E} e^{j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} \cos \theta_R} + \sum_{n \in \mathcal{E}_L(k)} e^{-j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_E} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} - \sum_{n \in \mathcal{O}_L(k)} e^{-j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_E} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos \theta_R} \right) + z_E(k) \\ = \underbrace{s(k)}_{\text{information symbol}} \underbrace{g_E \sqrt{P\alpha_E}}_{\text{effective channel gain}} \underbrace{\sqrt{N_E} \beta}_{\text{artificial noise}} + \underbrace{z_E(k)}_{\text{additive noise}}, \quad (7)$$

where α_E and g_E are the path loss and the channel gain at the eavesdropper, N_E is the eavesdropper's array gain, and $z_E \sim \mathcal{CN}(0, \sigma_E^2)$ is the additive noise at the eavesdropper. The term β in (7) is

$$\beta = \sqrt{\frac{1}{N_T}} \left(\sum_{m \in \mathcal{I}_M(k)} e^{j(\frac{N-1}{2}-m)\frac{2\pi d}{\lambda} (\cos \theta_R - \cos \theta_E)} + \sum_{n \in \mathcal{E}_L(k)} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos(\theta_R - \theta_E)} - \sum_{n \in \mathcal{O}_L(k)} e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} \cos(\theta_R - \theta_E)} \right). \quad (8)$$

Since the entries of $\mathcal{I}_M(k)$ and $\mathcal{I}_L(k)$ are randomly selected for each data symbol, (8) can be simplified to

$$\beta = \sqrt{\frac{1}{N_T}} \sum_{n=0}^{N_T-1} W_n e^{j(\frac{N-1}{2}-n)\frac{2\pi d}{\lambda} (\cos \theta_R - \cos \theta_E)}, \quad (9)$$

where W_n is a Bernoulli random variable and $W_n = 1$ with probability $(M + (N_T - M)/2)/N_T = \frac{N_T + M}{2N_T}$, and $W_n = -1$ with probability $\frac{N_T - M}{2N_T}$.

IV. PERFORMANCE EVALUATION

In this section, we evaluate the performance of the proposed mmWave secure transmission technique. As shown in (7), the received signal at an arbitrary eavesdropper is subject to both multiplication and additive noise. This makes the derivation of a simple closed form expression for the signal-to-noise ratio (SNR) and a secrecy rate formula challenging, if not possible. To evaluate the performance of the proposed mmWave secure transmission technique, we define the the secrecy throughput R (bits per channel use) as

$$R = [\log_2(1 + \gamma_R) - \log_2(1 + \gamma_E)]^+, \quad (10)$$

where γ_R is the SNR at the target receiver, γ_E is the SNR at the eavesdropper, and a^+ denotes $\max\{0, a\}$. From (3) and (6), the SNR at the receiver can be expressed as

$$\gamma_R = \frac{P\alpha N_R (\mathbb{E}[\mathbf{h}^*(\theta_R) \mathbf{f}(k)])^2}{P\alpha N_R \text{var}[\mathbf{h}^*(\theta_R) \mathbf{f}(k)] + \sigma^2} \quad (11)$$

$$= \frac{P\alpha N_R M^2 g_R^2}{N_T \sigma^2} = \frac{2P\alpha N_R M^2 \sin^2(\Phi_R/2)}{N_T \sigma^2}, \quad (12)$$

where (12) follows since the array gain is constant at the target receiver and $g_R^2 = \frac{1}{2}(1 - e^{-j\Phi_R})(1 - e^{j\Phi_R}) = (1 - \cos(\Phi_R)) = 2\sin^2(\Phi_R/2)$, and Φ_R is the phase angle between the receiver's direct and the reflected path.

Similarly, the SNR at an eavesdropper can be expressed as

$$\gamma_E = \frac{P\alpha_E N_E (\mathbb{E}[\mathbf{h}^*(\theta_E) \mathbf{f}(k)])^2}{P\alpha_E N_E \text{var}[\mathbf{h}^*(\theta_E) \mathbf{f}(k)] + \sigma_E^2} \quad (13)$$

$$= \frac{P\alpha_E N_E g_E^2 (\mathbb{E}[\beta])^2}{P\alpha_E N_E g_E^2 \text{var}[\beta] + \sigma_E^2}, \quad (14)$$

where $g_E^2 = 2\sin^2(\Phi_E/2)$, and Φ_E is the phase angle between the eavesdropper's direct and the reflected path. To derive γ_E , we need to characterize the random variable β in (9). Note that the random variable β is a sum of complex random variable. Invoking the central limit theorem, the artificial noise term β can be approximated by a complex Gaussian random variable for sufficiently large N_T , and, it can be completely characterized by its mean and variance. To complete the SNR derivation, we introduce the following lemma

Lemma 1: For large number of antennas N_T and $\theta_R \neq \theta_E$,

$$\mathbb{E}[\beta] = \frac{M}{N_T \sqrt{N_T}} \frac{\sin(N_T \frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E))}{\sin(\frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E))}, \quad (15)$$

and

$$\text{var}[\beta] \approx \frac{N_T^2 - M^2}{N_T^2}. \quad (16)$$

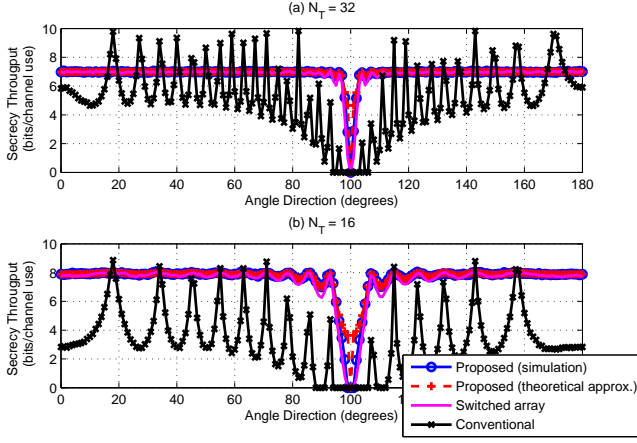


Fig. 3: Numerical and theoretical (eq. (18)) values of the secrecy throughput versus the eavesdropper's angular direction; (a) $N_T = 32$ and $M = 24$, (b) $N_T = 16$ and $M = 12$.

Proof: The proof can be found in [30] and is omitted for space limitation. ■

Using (15) and (16) γ_E in (14) becomes

$$\gamma_E \approx \frac{1}{\frac{N_T^2 - M^2}{N_T^2} + \frac{\sigma_E^2}{2P\alpha_E N_E \sin^2(\Phi_E/2)}} \times \left(\frac{M^2 \sin^2 \left(N_T \frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E) \right)}{N_T^3 \sin^2 \left(\frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E) \right)} \right), \quad (17)$$

where the approximation arises from (16).

Substituting (12) and (17) in (10), we obtain

$$R \approx \left[\log_2 \left(1 + \frac{2P\alpha_R M^2 \sin^2(\Phi_R/2)}{N_T \sigma^2} \right) - \log_2 \left(1 + \frac{1}{\frac{N_T^2 - M^2}{N_T^2} + \frac{\sigma_E^2}{2P\alpha_E N_E \sin^2(\Phi_E/2)}} \times \left(\frac{M^2 \sin^2 \left(N_T \frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E) \right)}{N_T^3 \sin^2 \left(\frac{\pi d}{\lambda} (\cos \theta_R - \cos \theta_E) \right)} \right) \right) \right]^+. \quad (18)$$

V. NUMERICAL RESULTS AND DISCUSSIONS

In this section, we consider vehicle-to-vehicle transmission and study the performance of the proposed security technique in the presence of an eavesdropper. For comparison, we simulate and plot the secrecy throughput of conventional array (without PHY security) and switched array [20] transmission techniques. Unless otherwise specified, the number of antennas at the transmitter is $N_T = 32$, $|g_R|^2 N_R = 8$, and $|g_E|^2 N_E = 32$. The system operates at 60 GHz with a bandwidth of 50 MHz and an average transmit power of 37 dBm. The distance from the transmitter to the receiver is 30 meters, the distance from the transmitter to the eavesdropper is 10 meters, and the path loss exponent is fixed to 2.

In Fig. 3, we plot the secrecy throughput achieved by the proposed technique versus the eavesdropper's angular location when using 32 and 16 transmit antennas. We also plot the secrecy throughput achieved by conventional array and switched transmission methods. In Figs. 3(a) and (b), we show

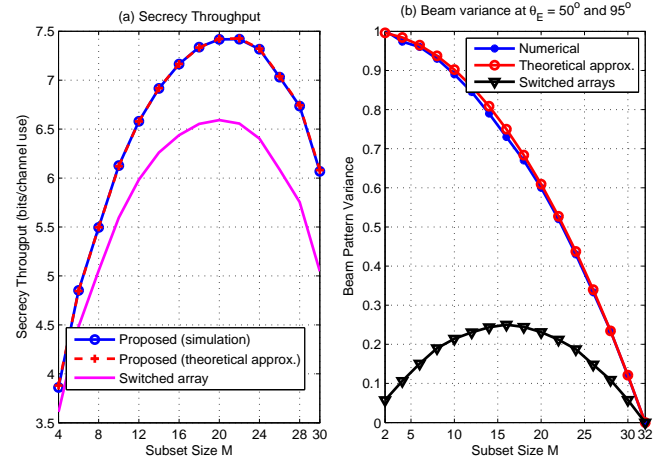


Fig. 4: (a) Numerical and theoretical (eq. (18)) values of the secrecy throughput versus the transmission subset size M ; $N_T = 32$, $\theta_R = 100^\circ$, and $\theta_E = 95^\circ$. (b) Beam variance at $\theta_E = 50^\circ$ and $\theta_E = 95^\circ$ (superimposed).

that the secrecy throughput of the proposed technique is high at all angular locations except at the target receiver's angular location ($\theta_R = 100$ degrees). We also show that switched array techniques provide comparable secrecy throughput with the proposed technique, while conventional array techniques provide poor secrecy throughputs, especially for lower number of transmit antennas as shown in Fig. 3(b). The reason for this is that conventional array transmission techniques result in a constant radiation pattern at the eavesdropper while, the proposed and the switched array techniques randomize the radiation pattern at an eavesdropper, thereby creating artificial noise. For the proposed and switched array transmission techniques, no randomness is experienced at the target receiver, and the secrecy throughput is minimum when the eavesdropper is located in the same angle with the target receiver, which is generally not the case in practice. We also observe that the proposed technique performs better than switched array techniques especially when the eavesdropper is closely located to the legitimate receiver, which is typically the worst case scenario.

In Figs. 4(a) and (b) we examine the impact of the transmission subset size M on the secrecy throughput and the generated beam pattern variance (or artificial noise). In Fig. 4(a), we observe that as the subset size M increases, the secrecy throughput of the proposed technique increases, plateaus, and then decreases. The reason for this is that as M increases, more antennas are co-phased for data transmission. On one hand, this increases the beamforming gain at the target receiver. On the other hand, increasing M decreases the variance of the artificial noise at the eavesdropper as shown in Fig. 4(b). Therefore, there is a trade-off between the beamforming gain at the receiver and the artificial noise at a potential eavesdropper, and there exists the optimum value of M that maximizes the secrecy throughput. In Figs. 4(a) and (b), we also show that the proposed technique provides higher secrecy throughput and beam pattern variance (or artificial

noise) when compared to the switched array technique without the need for additional antenna switches as required by the switched array technique. In the switched array technique, only M antennas are used to generate the artificial noise, while the remaining $N_T - M$ antennas are idle. The proposed technique uses $N_T - M$ antennas to generate artificial noise at potential eavesdroppers, and hence, results in higher secrecy throughput and artificial noise. In addition to reducing the beam pattern variance at a potential eavesdropper, the idle antennas create a sparse array which could be exploited to launch attacks on switched array techniques. Since the proposed technique uses all antennas, it is difficult to breach. Finally, in Fig. 4(a), we show that the theoretical approximation of the secrecy throughput is tight when compared to the secrecy throughput achieved by Monte Carlo simulation results. This enables us to gain further insights into the impact of key parameters such as, the subset size M and number of transmit/receive antennas, on the system performance.

VI. CONCLUSIONS

In this paper, we proposed a PHY layer security technique for secure mmWave vehicular communication. The proposed technique takes advantage of the large antenna arrays at the mmWave frequencies to jam eavesdroppers with sensitive receivers. This enhances the security of the communication link between a transmitter and a legitimate receiver. The proposed technique is shown to provide high secrecy throughput when compared to conventional and switched array techniques without the need for encryption/decryption keys and additional communication and processing overhead at the target receiver. This makes the proposed security technique favorable for time-critical road safety applications and vehicular communications in general.

ACKNOWLEDGEMENT

This research was partially supported by the U.S. Department of Transportation through the Data-Supported Transportation Operations and Planning (D-STOP) Tier 1 University Transportation Center and by the Texas Department of Transportation under Project 0-6877 entitled Communications and Radar-Supported Transportation Operations and Planning (CAR-STOP).

REFERENCES

- [1] J. Harding, G. Powell, R. Yoon, J. Fikentscher, C. Doyle, D. Sade, M. Lukuc, J. Simons, and J. Wang, *Vehicle-to-vehicle communications: Readiness of V2V technology for application*. (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration, Aug. 2014.
- [2] M. Raya, P. Papadimitratos, and J. Hubaux, "Securing vehicular communications," in *IEEE Wireless Commun.*, vol. 13, no. 5, pp.8-15, Oct. 2006.
- [3] M. Amoozadeh, A. Raghuramu, C. Chen-Nee, D. Ghosal, H. Zhang, J. Rowe, and K. Levitt, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," *IEEE Commun. Mag.*, vol.53, no.6, pp.126-132, June 2015.
- [4] A. Aijaz, B. Bochow, F. Dotzer, A. Festag, M. Gerlach, R. Kroh, and T. Leinmuller, "Attacks on inter vehicle communication systems - an Analysis," in *Proc. WIT*, 2006, pp. 189-194.
- [5] M. Gerlach, "Assessing and improving privacy in VANETs," in *Proc. of Fourth Workshop on Embedded Security in Cars*, Nov. 2006.
- [6] J. Hubaux, S. Capkun, and J. Luo, "The security and privacy of smart vehicles," *IEEE Security and Privacy Mag.*, vol. 2, no. 3, May 2004, pp. 49-55.
- [7] M. Raya and J. Hubaux, "The security of vehicular Ad hoc networks," *Proc. of ACM Workshop on Security of Ad Hoc and Sensor Networks*, Nov. 2005.
- [8] J. Guo, J. P. Baugh, and S. Wang, "A group signature based secure and privacy-preserving vehicular communication framework," in *Proc. Mobile Netw. Veh. Environ.* 2007, pp. 103-108.
- [9] A. Yener and S. Ulukus, "Wireless physical-layer security: lessons learned from information theory," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1814-1825, 2015.
- [10] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3088-3104, July 2010.
- [11] M. Daly and J. Bernhard, "Directional modulation and coding in arrays," in *Proc. 2011 IEEE Intl. Symp. Antennas Propag.*, pp. 1984-1987.
- [12] Y. Ding and V. Fusco, "Directional modulation transmitter radiation pattern considerations," *Microw., Antennas Propag.*, vol. 7, no. 15, pp. 1201-1206, Dec. 2013.
- [13] Y. Ding and V. Fusco, "Constraining directional modulation transmitter radiation patterns," *Microw., Antennas Propag.*, vol. 5, no. 18, pp. 1408-1415, Dec. 2014.
- [14] S. Goel, and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6 pp. 2180-2189, 2008.
- [15] J. Vilela, M. Bloch, J. Barros and S. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 256-266, June 2011.
- [16] T. Hong, M. Z. Song, and Y. Liu, "Dual-beam directional modulation technique for physical-layer secure communication," *IEEE Antennas Wireless Propag. Lett.*, vol. 10, 2011.
- [17] E. Baghdady, "Directional signal modulation by means of switched spaced antennas," *IEEE Trans. Commun.*, vol. 38, no. 4, Apr. 1990.
- [18] M. Daly and J. Bernhard, "Beamsteering in pattern reconfigurable arrays using directional modulation," *IEEE Trans. Antennas Propag.*, vol. 58, no. 7, July 2010.
- [19] N. Alotaibi, and K. Hamdi, "Switched phased-array transmission architecture for secure millimeter-wave wireless communication," in *IEEE Trans. Commun.*, no. 99, pp.1-1.
- [20] N. Valliappan, A. Lozano, and R. Heath, "Antenna subset modulation for secure millimeter-wave wireless communication," *IEEE Trans. Commun.*, vol. 61, no. 8, pp.3231-3245, Aug. 2013.
- [21] Z. Pi and F. Khan, "An introduction to millimeter-wave mobile broadband systems," *IEEE Commun. Mag.*, vol. 49, no. 6, pp. 101-107, June 2011.
- [22] A. Alkhateeb, O. Ayach, and R. W. Heath Jr, "Channel estimation and hybrid precoding for millimeter wave cellular systems," *IEEE J. on Select. Areas in Commun.*, vol. 8, no. 5, pp. 831-846, Oct. 2014.
- [23] V. Pellegrini, F. Principe, G. de Mauro, R. Guidi, V. Martorelli, and R. Cioni, "Cryptographically secure radios based on directional modulation," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 8163-8167, May 2014.
- [24] C. Rusu, N. Gonzalez-Prelcic, and R. Heath, "An attack on antenna subset modulation for millimeter wave communication," in *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 2914-2918, April 2015.
- [25] M. Akdeniz, Y. Liu, M. Samimi, S. Sun, S. Rangan, T. Rappaport, and E. Erkip, "Millimeter wave channel modeling and cellular capacity evaluation," *IEEE J. on Selected Areas in Commun.*, vol. 32, no. 6, pp. 1164-1179, June 2014.
- [26] M. Boban, W. Viriyasitavat and O. Tonguz, "Modeling vehicle-to-vehicle line of sight channels and its impact on application-layer performance," in *Proc. 10th ACM Int. Workshop VANET, Syst. Appl.*, Taipei, Taiwan, June 2013, pp. 91-94.
- [27] W. Schafer, "A new deterministic/stochastic approach to model the intervehicle channel at 60 GHz," in *Veh. Technol. Conf.*, Secaucus, NJ, May 1993, pp. 112-115.
- [28] W. Schafer, "Channel modelling of short-range radio links at 60 GHz for mobile intervehicle communication," in *Veh. Tech. Conf.*, St. Louis, Missouri, USA, May 1991, pp. 314-319.
- [29] H. L. Van Trees, *Optimum array processing (detection, estimation, and modulation theory, part IV)*, 1st ed. WileyInterscience, Mar. 2002.
- [30] M. Eltayeb, J. Choi, T. Al-Naffouri, and R. Heath, "Enhancing secrecy with multi-antenna transmission in millimeter wave vehicular communication systems," *in preparation*.